UCRL-CONF-214236

Measurements of Eavesdropping in a Wavelength/Time Optical CDMA (O-CDMA) System, with Data Confidentiality Implications

A. J. Mendez, V. J. Hernandez, C. V. Bennett, R. M. Gagliardi, W. J. Lennon

August 1, 2005

The 18th Annual Meeting of the IEEE Lasers & Electro-Optics Society (LEOS 2005)
Sydney, Australia
October 23, 2005 through October 27, 2005

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Measurements of Eavesdropping in a Wavelength/Time Optical CDMA (O-CDMA) System, with Data Confidentiality Implications

A. J. Mendez[a] , V. J. Hernandez*[b] , C. V. Bennett*, R. M. Gagliardi[c], and W. J. Lennon*
[a]*Mendez R&D Associates, P.O. Box 2756, El Segundo, CA 90245, Phone: (310) 640-0497, MendezRDA@AOL.com*
**Lawrence Livermore National Laboratory (LLNL), P.O. Box 808, L-229, Livermore, CA 94551;*
[b]*University of California at Davis, Department of ECE, Davis, CA 95616*
[c]*Department of EE-Systems, University of Southern California, Los Angeles, CA 90089-2565*

Abstract: We report measurements on what an eavesdropper "sees" when tapping into a wavelength/time O-CDMA system in which 16 of 32 codes are "lit". Severe multi-access interference (MAI) provides some data confidentiality.

1.0 Introduction

There are different positions with regards to how well O-CDMA supports secure communications. Tančevski [1] proposes that O-CDMA can provide a very large code space for secure communications; but recent analyses of current implementations of O-CDMA found that this may not provide a high degree of data confidentiality (Shake [2,3]). References [2],[3] in particular concentrated on analyses that followed *Kerckhoffs' principle* (i.e., that the eavesdropper/intruder knows all about the user's codes) and where the eavesdropper has tapped the encoded signal prior to it being comingled with MAI. Reference [2] applied this methodology to the cases of wavelength/time codes where the weight W is high (31 or 101) and where the code dimension n_c x n_λ is also high (961x31 and 10201x31); here n_c = number of time chips in the 2D code and n_λ = number of wavelengths in the code.

We've been developing wavelength/time (W/T) codes and an associated O-CDMA technology demonstrator (TD) with quite the opposite features (for reasons of spectral efficiency): $W = 4$ and n_c x n_λ = 8x8 [4],[5],[6]. At a large number of users, as in our experiments, the MAI is severe because the TD is based on optical orthogonal codes (OOCs) and intensity modulation/direct detection (IM/DD) and, thus, there are no cancelling terms. With this in mind, we proceeded to investigate the scenario in [2] wherein each user is assigned several codes that are used concurrently in order to assure that the eavesdropper is always confronted with MAI. The experiments described here answer: How many codes need to be assigned to each user to provide some degree of data confidentiality?

2.0 The O-CDMA TD, Its Characterization, and Eavesdropping Measurement Results

Three kinds of experiments were performed: a test configuration for characterizing the performance of an O-CDMA system; a test configuration to see whether O-CDMA is susceptible to eavesdropping when the MAI is severe (while the indended channel has very good BER performance and the number of concurrent codes, hence MAI, is very large); and a test configuration to see if the members of a code set can eavesdrop on each other.

The TD (see Fig. 1a) is the platform for these experiments; its W/T OOC codes, architecture, and IM/DD implementation with commercial-off-the-shelf components is described in [4],[5],[6]. The TD is designed for a codes set of 32 and, in these experiments, 16 of the 32 were "lit". The individual symbol rate is 1.25 Gsymbols/s, corresponding to Gigabit Ethernet; the chip rate is eight times this. Each symbol sequence is a 2^{31}-1 length pseudo random bit sequence (PRBS).

Fig. 1b shows eye diagrams of incoming decoded signals along with BER of the recovered data stream measured in the characterization of the TD. The back-to-back (B-B) case bypasses the encoders and decoder while the one user case disconnects all encoder outputs, except the output of encoder 9. Neglible penalty occurs between the B-B and single user cases. Subsequent users are added by reconnecting the encoder outputs in numerical order (i.e., Code 9, Code 10,…Code 24). The eye diagrams show that each user adds a MAI peak to the decoder ouput; these MAI peaks cluster around the signal. To keep eye open at a high number of users, coarse delays (~100 ps, the chip time) were applied to the seven interferers that tended to produce the worst beat interference, which results from all codes sharing the single encodable carrier (EC), our coherent multi-wavelength source. Beat interference significantly reduces if each user/encoder has its own EC source, or if a lower coherence source is used. The BER curves show that the power penalty per added interferer (minus its MAI power contribution) is only 0.18 dB. Even when the MAI tails leak into the sampling window and cause significant beat interference, a BER of less than 10^{-11} has been achieved with 16 users. The arrow at the end of the BER curves indicates the minimum power into the receiver module at which no errors occurred in the course of 100 billion bits.

We then used the TD to explore eavesdropping. Fig. 1c shows the BER and eye-diagrams in a scenario where an eavesdropper taps off a single wavelength of the encoded signal before the decoder to detect the signal based on the on-off-keying (OOK) aspect of the IM/DD codes, using the same receiver structure as shown in Fig. 1a. In all cases (one to sixteen users), a signal is indeed detectable with nontrivial BER, supporting Shake's analyses [2] and the need to add more MAI to increase the chaos of O-CDMA communications. Fig. 1d shows the BER for the eavsedropping by the Code 9 decoder, but with the real Code 9 signal turned off. In this scenario, a signal can be derived from the MAI of other users until the number of users exceeds four. Above four users, the encoders/decoder mismatch appears to distort and destablilize the intercepted signal, leading to a BER floor greater than 10^{-2}.

3.0 Summary and Conclusions

We measured the susceptibility to eavesdropping in a W/T IM/DD O-CDMA system. The ability for an intruder to eavesdrop with good BER is present, but degrades with number of users. More than 16 simultaneously "lit" codes per user is required to degrade the eavesdropping BER to worst than 10^{-2}. Members of a code set can eavesdrop on each other by means of MAI, but this capability is negligible when the number of concurrent users exceeds four.

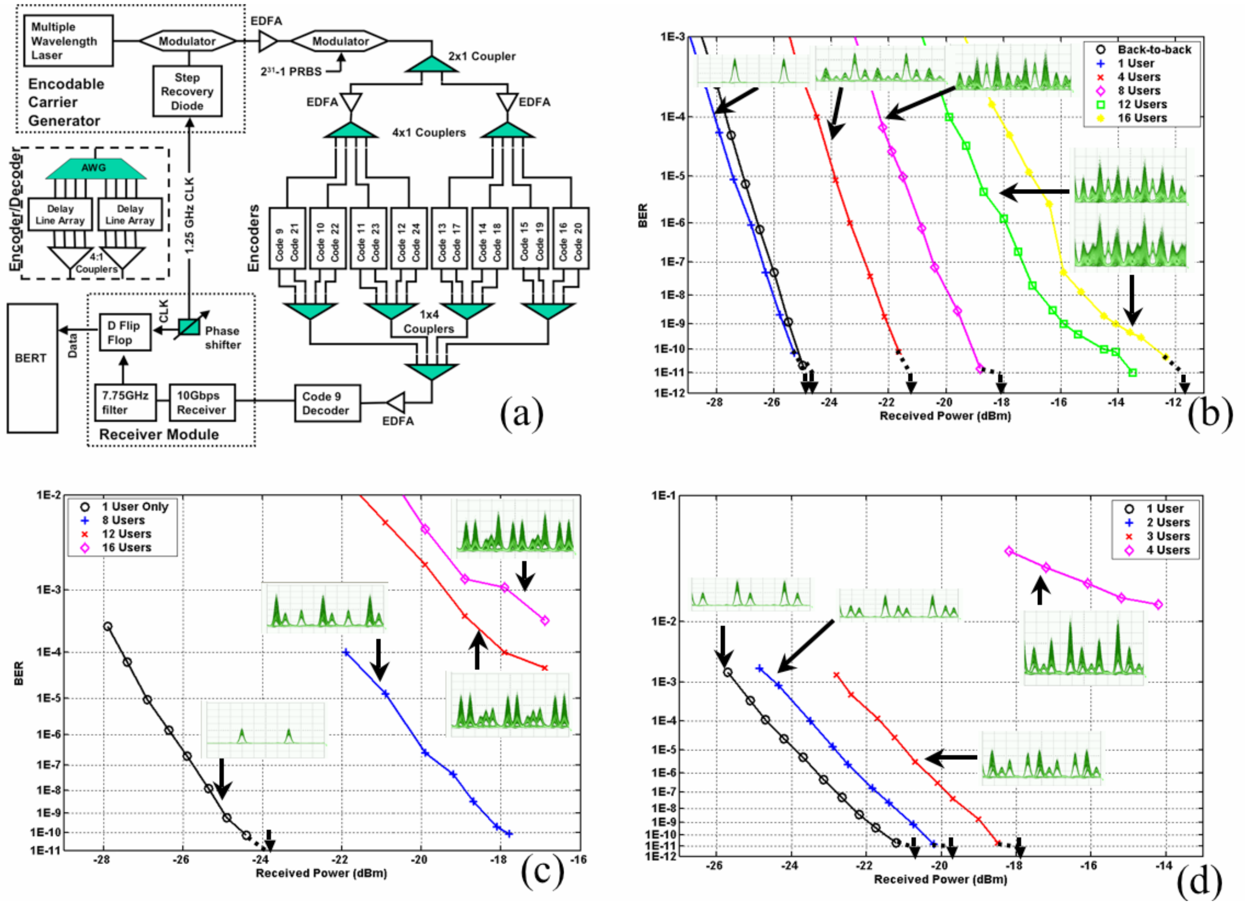

Figure 1: (a) Set-up for the sixteen user technology demonstrator. (b) BER and eye diagram measurements characterizing the O-CDMA TD for one to sixteen users. BER and eye diagram measurements for (c) classical eavesdropping and (d) eavesdropping on fellow codes.

Acknowledgments: This effort was supported in part by U.S. Department of Energy SBIR Phase II Grant ER83277 and performed under the auspices of the U.S. Department of Energy by the University of California LLNL under contract No. W-7405-Eng-48 and a subcontract to ER83277. The collaboration between MRDA and LLNL was carried out under Cooperative Research and Development Agreement TC-2051-02.

References

[1] L. Tančevski, I. Andonovic, and J. Budin; Secure optical network architectures utilizing hybrid wavelength hopping/time spreading codes. *IEEE Photonics Technol. Lett.* 7(5): 573-575 (1995).

[2] T. H. Shake; Security performance of optical CDMA against eavesdropping; *J. Lightwave Technol.* 23(2):655 – 670 (2005).

[3] T. H. Shake; Confidentiality performance of spectral-phase-encoded optical CDMA; *J. Lightwave Technol.* 23(4):1652 – 1663 (2005).

[4] A. J. Mendez, R. M. Gagliardi, V. J. Hernandez, C. V. Bennett, and W. J. Lennon; High Performance Optical CDMA System Based on 2D Optical Orthogonal Codes. *J. Lightwave Technol.* 22(11):2409 – 2419 (2004).

[5] V. J. Hernandez, A. J., Mendez, C. V. Bennett, and W. J. Lennon; Bit-Error-Rate Performance of a Gigabit Ethernet O-CDMA Technology Demonstrator (TD). Conf. Proc., 2004 IEEE/LEOS. Paper WE5:499-500.

[6] V. J. Hernandez, A. J. Mendez, C. V. Bennett, R. M. Gagliardi, and W. J. Lennon; A Sixteen-User, BER<10^{-11}, Optical-CDMA (O-CDMA) Technology Demonstrator (TD) Using Wavelength/Time Codes; to be published**,** *IEEE Photonics Technol. Lett.* 17 (TBD): pp. TBD (2005).